

## CLAIMS

1. A method for secure transmissions, the method comprising:  
2 determining a short term key for a message for transmission, the short  
term key having a short term key identifier;  
4 determining an access key for the message, the access key having an  
access key identifier;  
6 encrypting the message with the access key;  
forming an Internet protocol header comprising the short term key  
8 identifier; and  
transmitting the encrypted message with the Internet protocol header.
2. The method as in claim 1, wherein the short term key identifier comprises  
2 the access key identifier.
3. The method as in claim 2, wherein short term key identifier further  
2 comprises a security parameter index value.
4. The method as in claim 3, wherein the security parameter index value is  
2 a random number.
5. The method as in claim 1, wherein the short term key is calculated as a  
2 function of the short term key identifier and the access key.
6. The method as in claim 5, wherein the short term key identifier is  
2 calculated by encrypting the short term key identifier with the access key.
7. The method as in claim 1, wherein the Internet protocol header is part of  
2 an ESP header.

8. The method as in claim 7, wherein the Internet protocol header further  
2 comprises a second random number, the second random number having a  
random number identifier.
9. The method as in claim 8, wherein the short term key identifier comprises  
2 the access key identifier and the random number identifier.
10. The method as in claim 9, wherein short term key identifier further  
2 comprises a security parameter index value.
11. The method as in claim 10, wherein the security parameter index value is  
2 a random number.
12. The method as in claim 8, wherein the short term key is calculated as a  
2 function of the short term key identifier, the second random number, and the  
access key.
13. The method as in claim 12, wherein the short term key identifier is  
2 calculated by encrypting the short term key identifier and the second random  
number with the access key.
14. A method for secure reception of a transmission, the method comprising:  
2 receiving a short term key identifier specific to a transmission, the short  
term key identifier corresponding to a short term key;  
4 determining an access key based on the short term key identifier;  
encrypting the short term key identifier with the access key to recover the  
6 short term key; and  
decrypting the transmission using the short term key.
15. The method as in claim 14, further comprising:  
2 storing the short term key identifier and short term key in a memory  
storage unit.

16. The method as in claim 14, wherein the short term key identifier is  
2 comprised of a random number and an access key identifier associated with the  
access key.

17. The method as in claim 14, wherein encrypting the short term key  
2 identifier further comprises encrypting the short term key identifier and a random  
number with the access key to recover the short term key.

18. In a wireless communication system supporting a broadcast service  
2 option, an infrastructure element comprising:

a receive circuitry;

4 a user identification unit, operative to recover a short-time key for  
decrypting a broadcast message, comprising:

6 processing unit operative to decrypt key information; and

8 a mobile equipment unit adapted to apply the short-time key for  
decrypting the broadcast message, comprising:

10 memory storage unit for storing a plurality of short term keys  
and short term key identifiers.

19. The infrastructure element as in claim 15, wherein the user identification  
2 unit further comprises a second memory storage unit for storing a plurality of  
access keys and access key identifiers.

20. The infrastructure element as in claim 15, wherein the memory storage  
2 unit is a secure memory storage unit.

21. An infrastructure element for a wireless communication system,  
2 comprising:

means for receiving a short term key identifier specific to a transmission,

4 the short term key identifier corresponding to a short term key;

6 means for determining an access key based on the short term key  
identifier;

8 means for encrypting the short term key identifier with the access key to  
recover the short term key; and

means for decrypting the transmission using the short term key.

22. A digital signal storage device, comprising:

- 2 first set of instructions for receiving a short term key identifier specific to a  
transmission, the short term key identifier corresponding to a short
- 4 term key;
- second set of instructions for determining an access key based on the
- 6 short term key identifier;
- third set of instructions for encrypting the short term key identifier with the
- 8 access key to recover the short term key; and
- fourth set of instructions for decrypting the transmission using the short
- 10 term key.

23. A communication signal transmitted on a carrier wave, comprising:

- 2 a first portion corresponding to a short term key identifier, the short term  
key identifier having a corresponding short term key; and
- 4 a second portion corresponding to a transmission payload encrypted  
using the short term key.

24. The communication signal as in claim 23, wherein the short term key  
2 identifier comprises:

- a random number portion; and
- 4 an access key identifier corresponding to an access key.